様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 ２０ 日現在

機関番号：８２６３６
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８２６

研究課題名（和文）異業種データマイニング向けプライバシー保護機械学習メカニズムに関する研究開発

研究課題名（英文）R&D of Machine Learning Mechanism for Privacy Preserving Data Mining over Different Industries

研究代表者

王　立華（Wang, Lihua）

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・主任研究員

研究者番号：００４４７２２８

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：
本研究では、まず、プライバシー保護機械学習に必要な秘密計算技術であるセキュアな大小比較という準同型暗号方式を提案し、学習済みの決定木のモデルから学習用データが漏洩することを防ぐため、差分プライバシーを使ったアプローチを提案した。次に、同業種データ向けに多くの機械学習手法を汎用できるプライバシー保護連合学習フレームワークを構築し、特に勾配ブースティング決定木に基づく効率的な連合学習方式を設計した。当方式に基づいて継続学習、更に、欠損値補完の手法を拡張し異業種データ向け連合学習への展開について研究開発を行っている。
一連の研究成果は9件の国際会議や論文誌で採択されたほか、特許出願も行った。

研究成果の学術的意義や社会的意義
本研究の学術的意義は、セキュアな大小比較の準同型暗号方式と差分プライバシーの実現アプローチの提案により、機械学習におけるプライバシー保護の新たなアプローチを提示したことである。また、異業種データの安全な利用を促進する効率的なプライバシー保護連合学習フレームワークを構築し、効率性とプライバシー保護の両立を可能にした。社会的意義としては、ビッグデータの拡大に伴う個人情報漏洩を防ぎ、金融や医療分野での安心して利用できる効率的なAIサービスの提供を支援する。

研究成果の概要（英文）：
In this study, we first proposed a homomorphic encryption method called secure magnitude comparison, which is a secret computation technology necessary for privacy-preserving machine learning, and then proposed an approach using differential privacy to prevent training data from being leaked from a trained decision tree model. Next, we constructed privacy-preserving federated learning frameworks that can be used for many machine learning methods for data from the same industry, and in particular designed an efficient federated learning scheme based on the gradient boosting decision trees. We are conducting research and development on federated continuous learning based on this scheme, and further expanding the method of missing value imputation to apply it to the mechanism of federated learning for data from different industries.
With the above research results, we have published 9 papers in international conferences and journals, and have applied for a patent.

研究分野：情報学基礎

キーワード：プライバシー保護　連合学習　決定木　継続学習　差分プライバシー　匿名化

1．研究開始当初の背景

異業種データマイニングは属性値の標準化や、業種を跨るデータを活用するためにエッジコンピューティング技術が必須となる。エッジデバイスはローカルに保有する完全信頼できるものと外部に設置される攻撃されやすいものがある。2015 年にマイクロソフトの Nishanth Chandran らは【J. Cryptol. 28(4): 745-768 (2015)】で、「Almost-Everywhere Secure Computation with Edge Corruptions」の概念を紹介した。エッジデバイスを敵にアクセスされることを常に考慮すべきだ。

本研究課題では核心をなす三つの問題点が考えられ：まずは、既存の秘密計算技術をそのまま異業種データの解析に適用できない。例えば、準同型計算と大小比較暗号技術の融合問題や、異なる暗号方式を統合する問題は未解決である。次に、異業種データの標準化問題と同・異業種データ混在する場合柔軟に対応できる学習メカニズムの研究はまだ不十分である。最後は、秘密計算と機械学習の融合問題である。これまで、同業種データに向けた研究では、複雑計算の多項式近似、クライアント側の事前処理、サーバ側の並行計算などで解決策が考えられたが、異業種データを対象にする際にエッジコンピューティングも用いることとなり、認証可能な軽量暗号方式を考えなければならない。

2．研究の目的

全ての物が繋がる IoT 時代がやってくる中、異なる領域から膨大なデータが集約されている。例えば、高齢の親の健康状態、日常活動、家電の稼働状況など親の情報がマイクロデータセンターに集まったり、エッジコンピューティングによる分析結果がクラウドサーバに送信されたりする。また、金融、医療、交通などの情報がインターネットを通じてクラウドサーバに集約される。こちらのデータに対する機械学習やデータマイニングにより、新たなビッグデータサービスが創出されつつある。一方、個人情報や機微情報の漏洩防止などプライバシー保護が重要な課題である。本研究では、異業種データマイニング向け、実用的なプライバシー保護機械学習メカニズムの研究設計を目的とする。

3．研究の方法

研究分担者 1 名（AI・機械学習専門家）、国内外の協力研究者 6 名（情報セキュリティ専門家、AI・機械学習専門大学院生）の研究体制で、これまで同業種データマイニングに向けた研究成果をベースにして研究を展開し、四年間計画で下記三つの研究課題に取り組んでいく。

課題 1. [R2 年度～R4 年度] セキュアなクラウド・エッジコンピューティングに関する研究
課題 2. [R2 年度～R5 年度] プライバシー保護しつつ直・並列学習メカニズムの設計
課題 3. [R3 年度～R5 年度] オープンデータを使用して提案方式の高速実装と実用性評価

4．研究成果

下記の(1)と(5)は課題1に関する成果、(2)～(4)は課題2と3に関する成果である。

(1) 準同型暗号を用いた秘密計算： 暗号化された形式で 2 つの整数を比較することは、プライバシー保護データマイニングや、安全なオークションなどに役立つ。Tushar Kanti Saha らは、Ring-LWE 仮定に基づいて、実用的なアプローチ SK17 を提案した【NBiS 2017: 553-565】。これは、2 つのクライアント（1 つは復号鍵を持つ）がアウトソースのクラウドサーバを介してデータを公開することなく比較する三者間計算モデルに基づいて確立された。我々は、SK17 方式から効率、セキュリティ、柔軟性を向上させる 3 つの拡張スキームを提案した。最初のプロトコルを実装して、Kristin Lauter らが提案した Ring-LWE ベースの準同型暗号化スキーム【CCSW 2011: 113-124】を使用してその効率性を示し、他の 2 つのプロトコルに対して、理論的なセキュリティ分析と実用性の評価を行った（成果は国際会議 NBiS 2020、及び国内学会 EMM 研究会で発表）。

(2) プライバシー保護連合学習（PPFL）のフレームワーク： 連合学習は、複数の組織がデータを共有せずに協力し、全体のデータに対して機械学習を行うための重要な手法である。ニューラルネットワーク（例えば、深層学習）と勾配ブースティング決定木（GBDT）の両方で使用できるものを含む、連合学習におけるプライバシー保護技術について検討した。既存の PPFL システムの多くを網羅する二通りの中央サーバを介したプライバシー保護フレームワークを紹介して、公開されている金融、医療、IoT のデータセットを使用した実験を通じて、プライバシー保護連合学習の有効性と、現実のシナリオで高精度で、安全かつプライバシーを保護する機械学習システムを開発する可能性を実証した。調査結果は、連合学習システムの設計と実装でプライバシーを考慮することの重要性を強調し、プライバシー保護技術が効果的で実用的な機械学習システムの開発を可能にするために不可欠であることを示唆している。一方、中央サーバの代わりにブロックチェーンを用いた分散型連合学習メカニズムも構築し、GBDT ベースの具体的なシステムで実用性を評価した（成果は論文誌 IEICE Trans. Inf. Syst.、J. Inf. Process.、国際会議 ICONIP 2022、及び国内学会 SCIS 2023、EMM 研究会などで発表）。

(3) GBDT に基づく効率的な連合学習（eFL-Boost）： 連合学習がプライバシー保護機械学習ための最先端の技術として注目されているが、GBDT に導入される場合、十分な精度を維持しながら通信効率とセキュリティのバランスをとることは、未解決の問題のままであった。これまでの研究を展開し、eFL-

Boost という GBDT に基づく効率的な連合学習方式を提案した。これにより、精度の損失、通信コスト、および情報漏洩が最小限に抑えられる。提案されたスキームは、更新時にローカル計算（各組織によって個別に実行される）とグローバル計算（すべての組織によって協調的に実行される）の適切な割り当てに焦点を合わせている。木構造はグローバルな計算のために高い通信コストを負担することが知られているが、葉の重みはそのようなコストを必要とせず、精度に比較的大きく寄与することが期待される。従って、提案された eFL-Boost では、木構造は1組織でローカルに決定され、葉の重みは全ての組織のローカル勾配を集約することによってグローバルに計算される。具体的には、eFL-Boost は更新ごとに 3 回の通信（最も効率的な方法では 1 回の通信）のみを必要とし、プライバシーリスクの低い統計情報のみが他の組織に漏洩する。公開データセットのパフォーマンス評価（ROC AUC、ログ損失、および F1 スコア）を通じて、提案された eFL-Boost は、通信コストが低く、プライバシー保護を提供しないスキームと同等の既存のスキームを上回った（成果は論文誌 IEEE ACCESS、国際会議 ICONIP 2021、及び国内学会 SCIS 2023 で発表し、特許出願を行った）。

（4）GBDT に基づく継続学習や、異業種データ向け連合学習メカニズム： 金融、医療、交通などの個人に関する機微な情報を持っている複数組織で日々生成される分散データを継続的に学習して高性能を維持することができる、継続学習型連合学習について提案した。具体的には、高性能な継続学習を実現するためのリプレイ用データセットを過去の学習データから効率的に選択する手法を提案し、(3)で述べた eFL-Boost に組み込む。これにより、組織間で情報漏洩のリスクが低い統計情報のみを通信し、最適なリプレイ用データを選択することで、非定常データに対してもロバストな予測が可能となる。

一方、水平型連合学習で参加組織が所有する特徴量が一致しない場合、共通特徴量のみでモデル学習する必要があり、情報損失が問題となる。これを解決するため、本研究では、Xu Zhou らの敵対的生成ネットワーク【Knowl. Based Syst. 228: 107261 (2021)】を用いた連合学習手法を提案する。特定組織がもつ完全な特徴量に基づいて欠損補完する生成モデルを連合学習し、組織間で共有することで情報損失が軽減されことが期待される。実験により、提案する連合学習手法の有効性を検証する。本技術を異業種データ向け展開することによってプライバシーを保護しつつ直・並列学習メカニズムの構築につながる（成果は国内学会 SCI'24、ISEC-2024/3、FAN 2022、SCIS 2022 で発表し、FAN 2022 プレゼンテーション賞受賞）。

（5）データ匿名化と決定木の融合による差分プライバシーを実現： 学習済みの決定木のモデルから学習で利用したデータが漏えいすることを防ぐため、（乱択）決定木にサンプリングと剪定を適用することで差分プライバシーを満たすことを示した。本方式は、Ninghui Li らが提案した差分プライバシー【AsiaCCS 2012: 32-33】から着想を得たものである。彼らの提案は、機械学習ではなくデータセットのプライバシー保護に関する成果であり、そこでは、*k*-匿名化とサンプリングを組み合わせることで、差分プライバシーを満たすことが示されている。我々は決定木学習における枝刈りが *k*-匿名化と類似していることに注目し、属するデータ数が少なく識別リスクが高くなる葉を剪定することで、ラプラスノイズなどの雑音を加えることなしに差分プライバシーを満たす決定木が構築できることを示した。

また本研究では、匿名化技術と決定木の安全性に密接な関係があることを示した。まず、多くの研究がなされているデータ匿名化技術を使用して、学習された決定木から生じる情報漏洩の程度を評価できることを示した。次に逆に、データ匿名化技術を使用して、決定木を特定の攻撃に対して強化できることを示している。強化方法として、決定木に対して、*k*-匿名化に相当する操作と *l*-多様性に相当する操作を加えることで、一意性攻撃および同種攻撃に対するセキュリティを向上できることを示した。その手法として、2 つの決定木枝刈り手法を提案し、これらの手法の精度を実験的に評価した（成果は国際会議 ICONIP 2023、ICISSP 2024、及び国内学会 SCIS 2024、CSS 2023、SCIS 2023、SCIS 2021 で発表）。

おわりに：（課題1）セキュアなクラウド・エッジコンピューティングに関連研究として、上記述べた(1)の大小比較手法と(5)の決定木における差分プライバシーアプローチはそれぞれアウトソーシング計算を依頼されるとき、データの機密性の確保と学習済みのモデルからデータのプライバシー保護に役に立つ有用且つ汎用的な技術であり、同業種か異業種かに関わらずプライバシー保護機械学習方式の構築に適用可能である。（課題 2 と 3）プライバシーを保護しつつ直・並列学習メカニズムの設計と高速実装に関する研究として、(2)で提出した中央サーバ経由のプライバシー保護連合学習フレームワーク及びブロックチェーンを用いた承認技術により中央サーバなしの分散型の連合学習フレームワークは深層学習にも勾配ブースティング決定木にも適用できる。また、(2)の一例となりつつ(3)で紹介した eFL-Boost におけるローカル計算とグローバル計算の分配手法、及び(4)の動的サンプリング手法は、同業種か異業種かに関わらず適用可能である。特に、(4)の欠損値補完するための敵対的生成ネットワークを用いた連合学習手法は異業種データ向けのプライバシー保護学習メカニズムの構築手法のコア技術になる。

代表者と分担者により、社会展開のために上記の成果をまとめて、それぞれ他分野の国際会議や、国内学会で招待講演として、周知活動を積極的に行ってきた（国際会議 CIF'23、 国内学会 EMM 研究会、NICT サイバーセキュリティシンポジウム 2024、 及び 2023 年度日本 OR 学会関西支部シンポジウムで発表）。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　1件／うちオープンアクセス　9件）

１．著者名 PHONG Le Trieu、PHUONG Tran Thi、WANG Lihua、OZAWA Seiichi	４．巻 E107.D
２．論文標題 Frameworks for Privacy-Preserving Federated Learning	５．発行年 2024年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 2～12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2023MUI0001	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 WAKABAYASHI Ryousuke、WANG Lihua、NOJIMA Ryo、WASEDA Atsushi	４．巻 -
２．論文標題 Security Evaluation of Decision Tree Meets Data Anonymization	５．発行年 2024年
３．雑誌名 ICISSP 2024	６．最初と最後の頁 853～860
掲載論文のDOI（デジタルオブジェクト識別子） 10.5220/0012456600003648	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 NOJIMA Ryo、WANG Lihua	４．巻 CCIS 1963
２．論文標題 Differential Private (Random) Decision Tree Without Adding Noise	５．発行年 2023年
３．雑誌名 ICONIP (9) 2023	６．最初と最後の頁 162～174
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-99-8138-0_14	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 YAMAMOTO Fuki、OZAWA Seiichi、WANG Lihua	４．巻 10
２．論文標題 eFL-Boost: Efficient Federated Learning for Gradient Boosting Decision Trees	５．発行年 2022年
３．雑誌名 IEEE Access	６．最初と最後の頁 43954～43963
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.3169502	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 ASRORI Septiviana Savitri、WANG Lihua、OZAWA Seiichi	4．巻 LNCS 13625
2．論文標題 Permissioned Blockchain-Based XGBoost for?Multi Banks Fraud Detection	5．発行年 2023年
3．雑誌名 ICONIP 2022	6．最初と最後の頁 683～692
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-30111-7_57	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 KANAMORI Sachiko、ABE Taeko、ITO Takuma、EMURA Keita、WANG Lihua、YAMAMOTO Shuntaro、PHONG Le Trieu、ABE Kaien、KIM Sangwook、NOJIMA Ryo、OZAWA Seiichi、MORIAI Shiho	4．巻 30
2．論文標題 Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks	5．発行年 2022年
3．雑誌名 Journal of Information Processing	6．最初と最後の頁 789～795
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.30.789	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 ITOKAZU Kengo、WANG Lihua、OZAWA Seiichi	4．巻 -
2．論文標題 Outlier Detection by Privacy-Preserving Ensemble Decision Tree U sing Homomorphic Encryption	5．発行年 2021年
3．雑誌名 IJCNN 2021	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/IJCNN52387.2021.9534464	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 YAMAMOTO Fuki、WANG Lihua、OZAWA Seiichi	4．巻 LNCS 12533
2．論文標題 New Approaches to Federated XGBoost Learning for Privacy-Preserving Data Analysis	5．発行年 2020年
3．雑誌名 ICONIP 2020	6．最初と最後の頁 558～569
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-63833-7_47	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 WANG Lihua、SAHA Tushar Kanti、AONO Yoshinori、KOSHIBA Takeshi、MORIAI Shiho	４．巻 AISC 1264
２．論文標題 Enhanced Secure Comparison Schemes Using Homomorphic Encryption	５．発行年 2020年
３．雑誌名 Advances in Networked-Based Information Systems, NBiS 2020	６．最初と最後の頁 211～224
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57811-4_20	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計15件（うち招待講演　4件／うち国際学会　1件）

１．発表者名 松並 駿、王 立華、井上 広明、小澤 誠一
２．発表標題 敵対的生成ネットワークを用いた水平型連合学習における欠損データ補完
３．学会等名 第68回システム制御情報学会研究発表講演会（SCI'24）
４．発表年 2024年

１．発表者名 北野 優斗、王 立華、小澤 誠一
２．発表標題 継続学習型連合学習モデルにおける効率的なリプレイデータの選択
３．学会等名 IEICE Technical Report, ISEC2023-95 (2024-03)
４．発表年 2024年

１．発表者名 小澤 誠一
２．発表標題 組織間連合学習AIによる社会課題へのチャレンジ -銀行不正送金検知の取組み
３．学会等名 NICTサイバーセキュリティシンポジウム2024（招待講演）
４．発表年 2024年

１．発表者名
王 立華

２．発表標題
AIにおけるプライバシー保護を強化した連合学習

３．学会等名
第5回マルチメディア情報ハイディィイング・エンリッチメント研究専門委員会 EMM研究会（招待講演）

４．発表年
2024年

１．発表者名
伊藤 優策、王 立華、野島 良、早稲田 篤志

２．発表標題
決定木へのk-匿名性とl-多様性の適用

３．学会等名
2024年暗号と情報セキュリティシンポジウム（SCIS 2024）

４．発表年
2024年

１．発表者名
小澤 誠一

２．発表標題
AIによる特殊詐欺監視

３．学会等名
2023年度日本OR学会関西支部シンポジウム（招待講演）

４．発表年
2023年

１．発表者名
OZAWA Seiichi

２．発表標題
Privacy-Preserving Machine Learning for Big Data Analysis -How can we solve social issues using AI? -

３．学会等名
Chitose International Forum on Science & Technology 2023（CIF'23）（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
ASRORI Septiviana Savitri、WANG Lihua、OZAWA Seiichi

２．発表標題
BFL-Boost: Blockchain-based Federated Learning for Gradient Boosting to Enhance Security in Model Training

３．学会等名
2023年暗号と情報セキュリティシンポジウム（SCIS 2023）

４．発表年
2023年

１．発表者名
若林 亮輔、王 立華、野島 良、早稲田 篤志

２．発表標題
決定木と(k-)匿名化の関係について

３．学会等名
2023年暗号と情報セキュリティシンポジウム（SCIS 2023）

４．発表年
2023年

１．発表者名
野島 良、王 立華、菊池 浩明

２．発表標題
匿名化において差分プライバシーは十分に安全な指標になっているか？

３．学会等名
コンピュータセキュリティシンポジウム2023（CSS 2023）

４．発表年
2023年

１．発表者名
三浦 啓吾、井上 広明、金 相旭、王 立華、小澤 誠一

２．発表標題
動的サンプリングを用いた連合学習型勾配ブースティング決定木の継続学習

３．学会等名
第30回インテリジェント・システム・シンポジウム(FAN 2022)

４．発表年
2022年

１．発表者名
三浦 啓吾、王 立華、小澤 誠一

２．発表標題
動的サンプリングを使用した勾配ブースティング決定木の連合追加学習

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS 2022）

４．発表年
2022年

１．発表者名
糸数 健吾、王 立華、小澤 誠一

２．発表標題
準同型暗号を用いたプライバシー保護決定木アンサンブルによる外れ値検知

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS 2021）

４．発表年
2021年

１．発表者名
野島 良、王 立華

２．発表標題
k-匿名化と（乱択）決定木の融合について

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS 2021）

４．発表年
2021年

１．発表者名
山本 楓己、王 立華、小澤 誠一

２．発表標題
協調学習スキームを導入したプライバシー保護XGBoost

３．学会等名
コンピュータセキュリティシンポジウム2020（CSS 2020）

４．発表年
2020年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 協調学習システム及び協調学習方法	発明者 王 立華、山本 楓己、小澤 誠一	権利者 情報通信研究機構、神戸大学
産業財産権の種類、番号 特許、特願2020-217245	出願年 2020年	国内・外国の別 国内

〔取得〕　計0件

〔その他〕

Home page
https://sfl.nict.go.jp/people/lihua-wang.html

DBLP 王立華
https://dblp.org/pid/28/2290-1.html

NICT サイバーセキュリティ研究所 セキュリティ基盤研究室
https://www.nict.go.jp/security/index.html

NICTの研究成果 発表論文一覧
https://www.nict.go.jp/outcome/papers/

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	小澤　誠一 (OZAWA Seiichi) (70214129)	神戸大学・数理・データサイエンスセンター・教授 (14501)	

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	野島　良 (NOJIMA Ryo)		
研究協力者	早稲田　篤志 (WASEDA Atsushi)		

6．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	山本　楓己 (YAMAMOTO Fuki)		
研究協力者	三浦　啓吾 (MIURA Keigo)		
研究協力者	北野　優斗 (KITANO Yuto)		
研究協力者	松並　駿 (MATSUNAMI Shun)		

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
バングラデシュ	Jatiya Kabi Kazi Nazrul Islam University			